(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 758 776 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.02.1997 Bulletin 1997/08

(51) Int Cl.[6]: **G07C 9/00**

(21) Application number: **96305458.0**

(22) Date of filing: **25.07.1996**

(84) Designated Contracting States:
DE ES FR GB IT

(30) Priority: **14.08.1995 GB 9516611**

(71) Applicant: **NCR International, Inc.**
Dayton, Ohio 45479 (US)

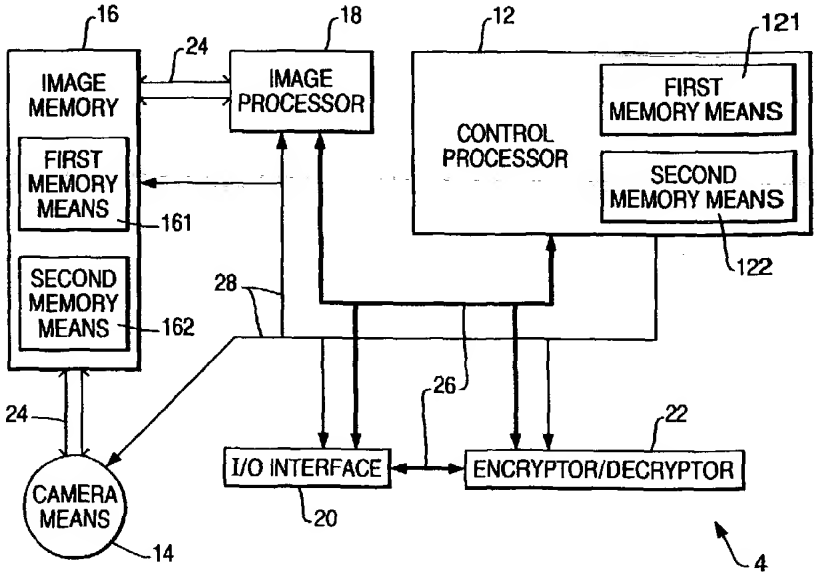
(72) Inventor: **Massie, Stephen Andrew**
Monikie Broughty Ferry, Dundee, DD5 3QG (GB)

(74) Representative: **Robinson, Robert George**
International Intellectual Property Department,
NCR LIMITED,
915 High Road,
North Finchley
London N12 8QJ (GB)

(54) An authorization system

(57) The invention relates to an authorisation system (2), characterized by an integrated circuit card (4) which incorporates camera means (14), data processing means (12,18), and memory means (161) in which is stored at least one digital image of an authorised user of the system. The card (4) is separable from a host means (6), when not in use. Communication means (20,21) are arranged to ensure encrypted communications between the card (4) and the host means (6). The camera means (14) is arranged to produce an image of a user and to forward this image to the processing means (18) for comparison with the or each image of an authorised user stored in the memory means (161). The processing means (18) produces a signal indicative of the result of the comparison, which is communicated in an encrypted form to the host means (6).

FIG. 3A



Printed by Jouve, 75001 PARIS (FR)

Description

The present invention relates to an authorisation system for authorising a person to carry out some predetermined action or procedure.

The invention has application, for example, as part of an access control system which in use controls the access of persons to a secure area or to a financial facility such as an automated teller machine (ATM).

With a view to improving the security of authorisation systems, it is known to provide biometric identification means. Known biometric identification means include, for example, finger print or hand print recognition systems, incorporating a digitiser which a user touches with his finger or hand, thus producing data characteristic of the user's finger or hand print. This data is compared with stored data characteristic of the finger or hand prints of persons who are authorised to use the system, and a signal indicative of the result of the comparison is produced.

Such systems have a drawback that a finger or even a hand print can be duplicated. Thus, an unauthorised person could replicate the hand or finger print of an authorised person and could falsely obtain access to an area or facility using a duplicate hand or finger print replicated, for example, on a synthetic glove.

It is an object of the present invention to provide an authorisation system having a high degree of security.

According to the present invention there is provided an authorisation system, characterized by an integrated circuit card which is arranged, when in use, to be removably mounted on a host means adapted to receive confirmation of the identity of a person using said card, and which incorporates: memory means arranged to have stored therein at least one reference image of the face of at least one person authorised to use said card, data processing means, and camera means arranged to produce an image of the face of a user of said card and to forward said image of said user to said data processing means for comparison with the or each reference image, said data processing means being arranged to produce a signal indicative of the result of said comparison; and communication means included in said card and said host means for providing communication therebetween, whereby said signal may be transmitted to said host means.

It should be understood that by an integrated circuit card is meant a card in which is embodied one or more integrated circuits.

An advantage of the present invention is that it is more difficult for an unauthorised person to obtain fraudulent access to an area or a facility than it would be with known biometric systems, because an image of an authorised user's face is utilized, which is more difficult to duplicate than that of an authorised user's finger or hand print.

Another advantage of the invention is that the image capture, reference image storage and comparison therebetween are carried out in a single device, namely the integrated circuit card, thereby reducing the likelihood of an unauthorised user of the integrated circuit card being able to interfere with the communication between the elements which carry out these functions, in an attempt to tamper with the system.

An embodiment of the present invention will now be described, by way of example, with reference to the accompanying drawings, in which:-

Fig. 1 is a perspective view of an authorisation system in accordance with the present invention, in use;
Fig. 2A is a front view of an integrated circuit card for use in the authorisation system of Fig. 1;
Fig. 2B is a rear view of the integrated circuit card of Fig. 2A;
Fig. 3A is a block circuit diagram of the integrated circuit card of Figs. 2A and 2B; and
Fig. 3B is a block circuit diagram of a host means utilized in the system of Fig. 1.

With reference to Fig. 1 there is illustrated an embodiment of an authorisation system 2 in accordance with the present invention. The authorisation system 2 incorporates: an integrated circuit card 4, incorporating a camera means 14 (Fig. 3A) having a lens 15, and a host means 6 connected to a door actuation device 8 which is controlled to unlock a door 10 providing access to a secure area for a person 11. The actuation device 8 unlocks the door 10 only when instructed to do so by the host means 6, on confirmation by the card 4 of the identity of the person 11.

The card 4 has main dimensions similar to those of a standard magnetic stripe card, the card 4 being approximately 85 millimetres x 55 millimetres in size with a thickness of 1.5 to 5 millimetres. The card 4 is separable from the host means 6 and is normally carried by a user, when not in use.

When a user wishes to operate the authorisation system 2 he or she inserts the card 4 into a grooved guide 5 in the host means 6. As illustrated in Fig. 1, the card 4 is inserted into the grooved guide 5 such that the camera lens 15 points outwards towards the user, in order to produce an image of the user. The card 4 and the grooved guide 5 are dimensioned so that the card 4 is held firmly in the grooved guide 5, so as to prevent "camera shake".

Referring now additionally to Fig. 3B, the host means 6 incorporates a power supply 13. When the card 4 is inserted into the grooved guide 5 (Fig. 1), the card 4 is connected to the power supply 13 via a contactless integrated circuit card power terminal 7 (Fig. 2B) on the opposite side of the card 4 from the camera lens 15 and via a corresponding contactless integrated circuit power terminal 9 on the host means 6. The card 4 also includes data communication terminals 19 (Fig. 2B), located adjacent the power terminal 7, which co-operate with cor-

respondingly located communication terminals 21 on the host means 6, for the transmission of data between the card 4 and the host means 6.

Inductive contactless connection is used because inductive transfer mechanisms require less accurate location of the terminals 7, 19 on the card 4 with respect to the terminals 9, 21 in the host means 6 than would be the case with non-inductive transfer mechanisms.

Referring particularly to Fig. 3A, the card 4 incorporates: a control processor 12, which controls the operation of the card 4; the camera means 14, which is in the form of a digital integrated circuit chip camera, used to produce a digital image of a user; and an image memory 16, comprising a first memory means 161 in which a digital image of the face of at least one person who is authorised to use the card 4 is stored, and a second memory means 162, in the form of a standard data buffer, in which the digital image produced by the camera means 14 is stored temporarily when the card 4 is in use. The card 4 also incorporates an image processor 18 in which data from the first and second memory means 161, 162 can be compared, and an input/output (I/O) interface 20 incorporating the contactless communication terminals 19, the interface 20 enabling communication between the card 4 and the host means 6. The card 4 further incorporates an encryptor/decryptor 22, arranged to encrypt signals from the card 4 prior to transmission to the host means 6 and to decrypt encrypted signals received from the host means 6.

The camera means 14 incorporates a charge coupled device (CCD) chip capable of storing an image of at least 200 by 200 pixels resolution. As will be known to a person skilled in the art, a CCD camera operates by focusing light onto the surface of each CCD element in the device, a charge being built up on each element at a predetermined rate. The image of a card user is "taken" by sampling the state of each CCD element by transferring the charge on the element to an associated charge measurement device, at a predetermined time. This sampling is analogous to the opening and closing of the shutter in a conventional camera.

Clearly, a low charge corresponds to a dark area in the image and a high charge to a light area. If the sampling speed is too low then over exposure can result, just as in an ordinary camera when too long an exposure time is used. Conversely, if too high a sampling rate is used there is not enough time for charges representative of an image to build up on the CCD elements and an under exposed image is produced. A sampling rate of 50 samples per second is considered to be optimum.

In use, the digital image of the head and shoulders of the user produced by a first sample is stored in a first "shadow" memory (not shown) in the camera means 14 and a second sample is taken, the image produced from this sample being stored in a second "shadow" memory (not shown). The camera means 14 compares the first and second images, pixel by pixel, in an analog difference array. This process ensures that fluctuations produced by slight movements of the user during the imaging process are compensated for by the camera means 14. This process is continued until the difference between two images is less than a predetermined maximum, and the last image is taken to be stable. This image is then converted into a digital bit stream by the camera means 14 and transmitted from the camera means 14 along a data bus 24 in the card 4 to the image memory 16 (Fig 3A).

If the card 4 is in a so-called authorised image registration mode (in which an image of an authorised user is to be stored in the card 4) when the image is produced, then the image is transferred to the first memory means 161 in the image memory 16. If the card 4 is not in the authorised image registration mode at the time the image is produced, then the image is transmitted to the second memory means 162 in the image memory 16, where it is held temporarily until it can be transferred to the image processor 18 for comparison with the image of the authorised user from the first memory means 161.

The control processor 12 included in the card 4 also incorporates a first memory means 121 in which is stored a secure "image registration" code which must be received by the card 4 before it will enter the authorised image registration mode. The control processor 12 also incorporates a second memory means 122 in which is stored a secure "card authorisation" code which must be transmitted to a processor 38 (Fig. 3B) in the host means 6 to confirm that the card 4 is authorised for use with the host means 6 prior to operation of the card 4, as will also be discussed further below.

Data is transmitted between the control and image processors 12, 18, the I/O interface 20 and the encryptor/decryptor 22 in the card 4 via data buses 26. The control processor 12 is also connected to the other components in the card 4 via control buses 28, through which the control processor 12 sends control signals to the other components of the card 4.

The procedure carried out by an authorised user to store his or her image in the first memory means 161 is as follows. The card 4 is inserted into the grooved guide 5 in the host means 6 and is thus connected to the power supply 13, as discussed above. The authorised user then uses a key pad 30 (Fig. 1) on the host means 6 to input the image registration code into the card 4, via the I/O interface 20.

The host means 6 includes a processor 38 (Fig. 3B), which in turn includes an encryptor/decryptor 40 which encrypts the image registration code entered by the authorised user prior to transmitting it to the card 4 via the I/O interface 20 (and encryptor/decryptor 22) and on to the control processor 12 via the data bus 26, thus reducing the likelihood of the code being detected by an unauthorised user.

When the image registration code is transmitted to the control processor 12 in the card 4 it is compared with the code stored in the first memory means 121 in the control processor 12. If the code entered by the user

corresponds to that stored in the first memory means 121 then, after a short delay as detailed below, the card 4 will enter the authorised image registration mode. This is indicated to the user by the illumination of a first light emitting diode (LED) 32 (Fig. 1) on the host means 6, which will remain illuminated until the image of the authorised user has been stored in the first memory means 161 in the memory 16. If the code entered by the user does not correspond to the code stored in the first memory means 121 in the control processor 12 the card 4 will not enter the authorised image registration mode, which will be indicated to the user by the failure of the first LED 32 to become illuminated.

After inserting the card 4 into the groove 5 the user then moves to a position approximately 1 metre to 1.5 metres in front of the card 4 and awaits the entry of the card 4 into the authorised image registration mode. The control processor 12 will instruct the camera means 14 to enter the authorised image recognition mode approximately three seconds after the card 4 is entered into the grooved guide 5 in the host means 6. This delay is preset in the control software in the control processor 12, in order to give the user time to be positioned in front of the camera means 14. The actual delay may be altered by altering this parameter in the software.

The software in the control processor 12 also includes a pattern recognition algorithm which is configured to look for an outline which conforms to the head and shoulders of a prospective user. If the pattern recognition algorithm has not confirmed that a person is standing in front of the camera means 14 by the end of the three second delay, the control processor 12 will not cause the card 4 to enter the authorised image recognition mode. Only after the pattern recognition algorithm has determined that a person is standing in front of the camera means 14 will the control processor 12 instruct the camera means 14 to enter the image recognition mode.

As the system is designed to allow different levels of access to different users, the first memory means 121 in the control processor 12 contains a plurality of different codes, each corresponding to a different level of access within the system. The access provided to a particular user is therefore dependent on the code which is entered prior to the user's image being entered into the first memory means 161 in the image memory 16 as an authorised user.

Once an appropriate authorisation code has been accepted by the card 4, the camera means 14 will produce an image of the authorised user and transfer it to the first memory means 161 in the image memory 16, in the manner detailed above.

When in use to gain access to the secure area, the card 4 is inserted by a user into the grooved guide 5 in the host means 6 connected to the door actuation means 8, as discussed above. The user then again stands approximately 1 metre to 1.5 metres in front of the card 4, in the host means 6. As with the aforementioned authorised image registration mode, the insertion of the card 4 into the grooved guide 5 connects the card 4 to the power supply 13. The control processor 12 then retrieves the card authorisation code stored in the second memory means 122 in the control processor 12 and forwards the code to the encryptor/decryptor 22 for encryption prior to transmitting the code to the host means 6 via the I/O interface 20. The card authorisation code is decrypted by the encryptor/decryptor 40 and compared in the processor 38 in the host means 6 with the code stored in the memory means 42 in the host means 6, before the host means 6 will accept the card 4 for operation. If the code transmitted by the card 4 corresponds to that required by the host means 6, the host means 6 will transmit an encrypted signal to the control processor 12, via the I/O interface 20, informing the control processor 12 that the card 4 is authorised for use in the host means 6.

If the system is configured such that the same host means 6 is utilised in the image registration mode, discussed above, as is used in user identification and authorisation then this card acceptance process is also undertaken by the host means 6 prior to the image registration process, to ensure that the card 4 is one which was issued for use with the particular authorisation system to which the host means 6 belongs.

The control processor 12 will then activate the camera means 14 to produce an image of the user standing in front of the card 4, in the manner discussed above. The camera means 14 will then forward the image to the image processor 18, via the second memory means 162 in the image memory 16. At this time the image of the authorised user is also forwarded from the first memory means 161 in the image memory 16 to the image processor 18, via the data bus 24, for comparison with the image produced by the camera means 14.

If the image of the user produced by the camera means 14 corresponds to that of the authorised user stored in the first memory means 161 then the image processor 18 will produce a first signal, indicative of this match, which is encrypted by the encryptor/decryptor 22 and transmitted, via the I/O interface 20, to the processor 38 in the host means 6, via the encryptor/decryptor 40. On receipt of the decrypted signal the processor 38 will produce and encrypt a corresponding signal which it will transmit to the door actuation device 8. On receipt of this signal from the processor 38 the door actuation device 8 unlocks the door 10 and a second LED 34 (Fig. 1) on the host means 6 is illuminated by the processor 38 in the host means 6, to indicate to the user that the door 10 has been unlocked. The user can then remove the card 4 from the host means 6 and open the unlocked door 10, which will remain unlocked for a predetermined period of time or until the door has been opened and closed once.

However, if the image of the user produced by the camera means 14 does not correspond to that of an authorised user read from the first memory means 161 in

the image memory 16 then the image processor 18 produces a second signal which is transmitted to the host means 6. On receipt of the second signal from the card 4 the processor 38 does not send a signal to the door actuation means 8, but instead causes a third LED 36 (Fig. 1) on the host means 6 to be illuminated, to indicate that the system has not recognised the user as an authorised user. The user must then remove the card 4 from the host means 6. Ideally the second LED 34 is green and the third LED 36 is red.

It should be understood that the first memory means 161 in the image memory 16 may include images of a plurality of authorised users, if the card 4 is intended for use by more than one person. For example, if the card 4 is to be used by a pool of authorised cleaning staff, the first memory means 161 will contain the images of each of these authorised users and the card 4 will be handed between them as required.

In this case, when the card 4 is in use, the image of the user is compared with the image of each authorised user in turn and the card 4 accepts the user as an authorised user if the user's image corresponds to that of any of the authorised user images stored in the first memory means 161.

The invention is not limited to use with door entry systems and can be utilized with other systems or apparatus where confirmation of a user's authorisation to use a card is required, including, for example, automated teller machines (ATMs).

Claims

1. An authorisation system (2), characterized by an integrated circuit card (4) which is arranged, when in use, to be removably mounted on a host means (6) adapted to receive confirmation of the identity of a person using said card, and which incorporates: memory means (161) arranged to have stored therein at least one reference image of the face of at least one person authorised to use said card, data processing means (12,18), and camera means (14) arranged to produce an image of the face of a user of said card and to forward said image of said user to said data processing means (12,18) for comparison with the or each reference image, said data processing means (12,18) being arranged to produce a signal indicative of the result of said comparison; and communication means (20,21) included in said card (4) and said host means (6) for providing communication therebetween, whereby said signal may be transmitted to said host means (6).

2. An authorisation system according to claim 1, characterized by memory means (122) in said card (4) in which is stored a first card authorisation code, which in use is transmitted to data processing means (38) in said host means (6) for comparison with a second card authorisation code stored in memory means (42) in said host means (6), the acceptance of said card (4) for use with said host means (6) being dependent on the result of said comparison of said first and second card authorisation codes.

3. An authorisation system according to claim 1 or claim 2, characterized by memory means (121) in said card (4) in which is stored a first image registration code, said first image registration code being compared, in use, in said data processing means (12,18) in said card (4) with a second image registration code input by a user of the system (2) via input means (30) in said host means (6), whereby, depending on the result of the comparison of said first and second image registration codes, said card (4) enters an image registration mode in which an image of the face of the user is stored in said memory means (161) as an image of an authorised user.

4. An authorisation system (2) according to any one of the preceding claims, characterized by first encryptor/decryptor means (22) located in said card (4) and second encryptor/decryptor means (40) located in said host means (6,8), said encryptor/decryptor means (22,40) being arranged to ensure encrypted communication between said card (4) and said host means (6).

5. An authorisation system according to any one of the preceding claims, characterized in that said host means (6) includes a power supply (13) to which said card (4) is connected when said card (4) is mounted on said host means (6).

6. An authorisation system according to claim 5, characterized in that said power supply (13) is arranged to supply power to said card (4) via contactless inductive terminals (7) provided on said card (4) and corresponding contactless inductive terminals (9) provided on said host means (6).

7. An authorisation system according to any one of the preceding claims, characterized in that said communications means (20) includes contactless inductive terminals (19) on said card (4), which cooperate with corresponding contactless inductive terminals (21) on said host means (6) when said card (4) is mounted on said host means (6).

8. An authorisation system according to any one of the preceding claims, characterized in that said camera means (14) incorporates a digital camera comprising a charge coupled device (CCD) integrated circuit chip.

9. An authorisation system according to any one of the

preceding claims, characterized in that said host means (6) is connected to an automated door entry device (8), said host means (6) being arranged to cause said device (8) to unlock a door (10), when said image of the user corresponds to an image of an authorised user stored in said memory means (161).

10. An integrated circuit card (4) adapted for use in an authorisation system according to any one of the preceding claims.

11. A host means (6) adapted for use in an authorisation system according to any one of claims 1 to 9.

FIG. 1

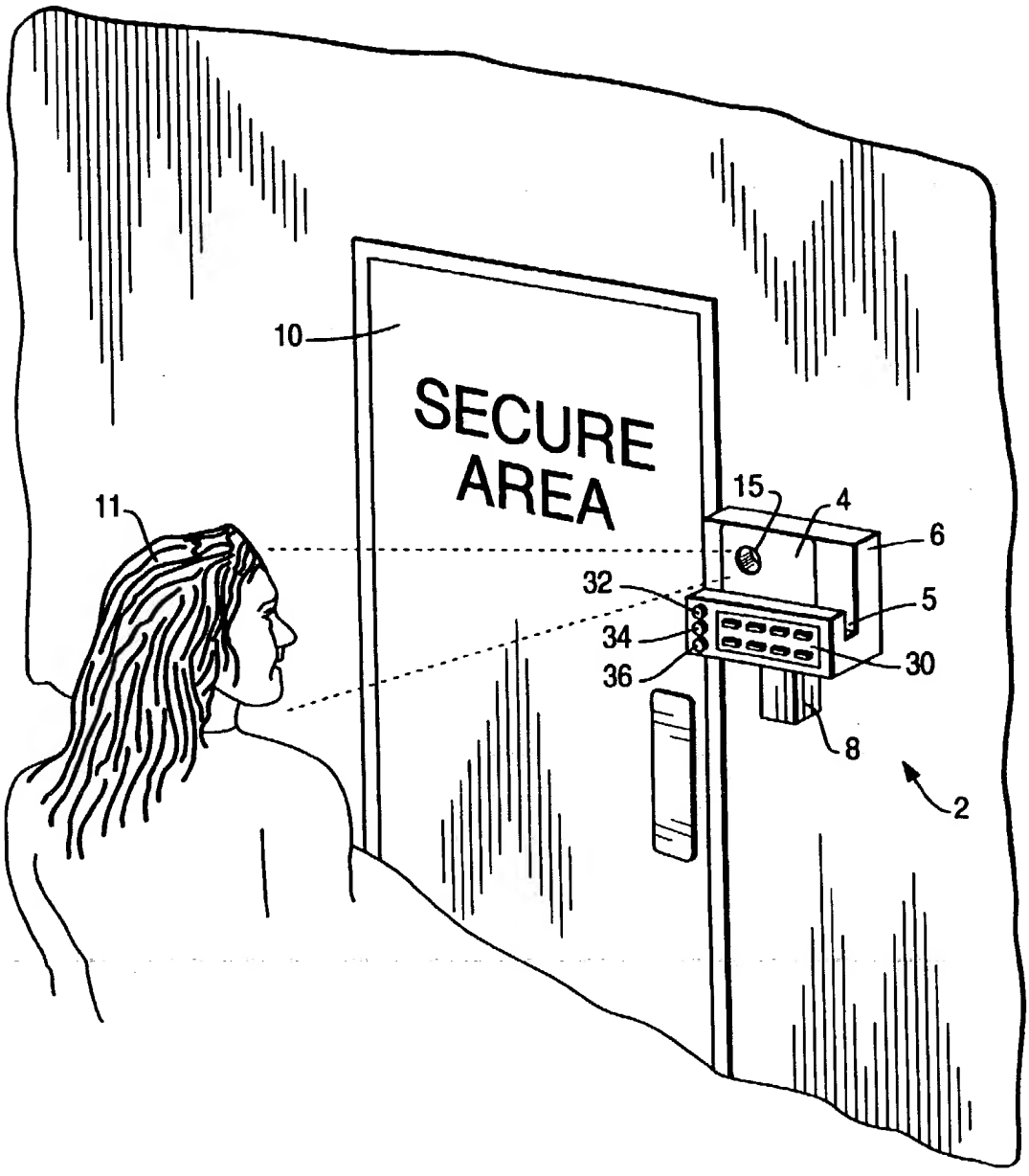


FIG. 2A

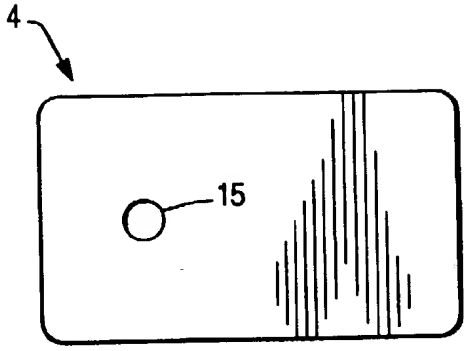


FIG. 2B

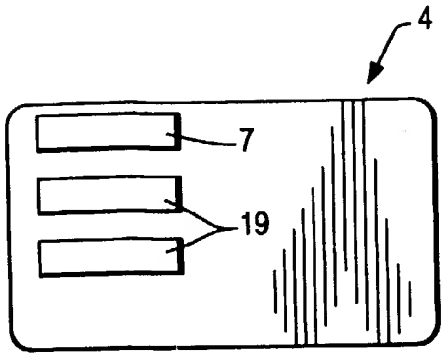


FIG. 3A

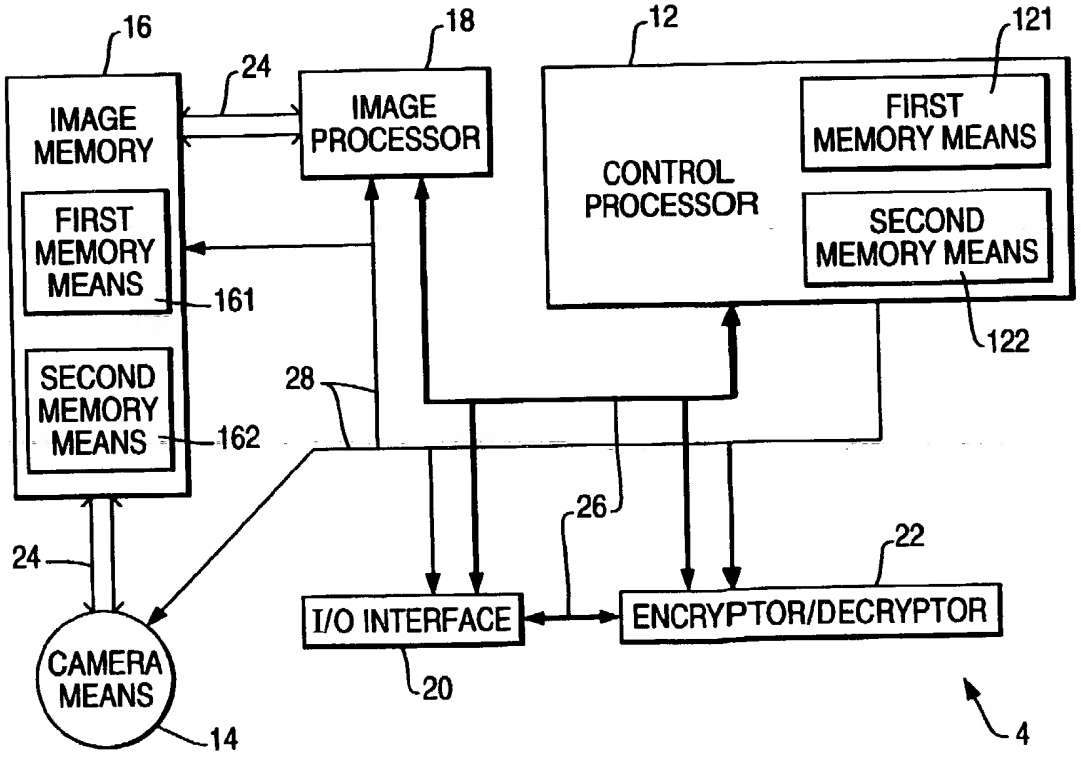


FIG. 3B